MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Metodické nástroje pro přípravu na obecné nařízení o ochraně osobních údajů

Školení pro zástupce obcí
duben 2018

Přehled metodických nástrojů

Ministerstvo vnitra zveřejnilo metodické nástroje, které jsou k dispozici obcím podle jejich konkrétní situace:

- checklisty pro malé obce,
- systémové analýzy – podávají návod na provedení analýzy rizik a nabízejí doporučená řešení modelových situací,
- metodika ke spisovým službám,
- vzorové dokumenty – záznamy o činnostech zpracování, směrnice o zpracování osobních údajů,
- metodika ke jmenování pověřence pro ochranu osobních údajů.

Checklisty

Dokument je zamýšlen jako základní materiál, který má poskytnout počáteční orientaci odpovědných osob v malých obcích ohledně systémových požadavků obecného nařízení o ochraně osobních údajů.

Obsahuje 3 základní listy

- "Úvod a doporučení",
- "Obecný seznam“, který obec provede po opatřeních, jimž je potřeba věnovat pozornost,
- "Seznam ke zpracování osobních údajů„, jenž lze využít při vlastní inventuře agend, kde se zpracovávají osobní údaje.

I. Nastavení kompetencí

V obci musí být určena osoba, která se věnuje níže uvedeným otázkám a zodpovídá za jejich řešení.
Má tedy odpovídající činnosti v popisu práce, popřípadě jí vyplývají z vnitřního předpisu nebo pokynu.

01. Stanovení prostředků (manuální/elektronické) zpracování osobních údajů.

02. Stanovení účelů zpracování (proč se údaje zpracovávají).

03. Posouzení, které osobní údaje je nutno shromažďovat.

04. Stanovení opatření, která omezí zpracování na minimální nutný rozsah.
(Např. nastavení kamery, základní dobu uložení údajů atd.)

05. Stanovení opatření, která prakticky chrání soukromí dotčených osob.
(Např. úroveň zabezpečení, rozsah sdělování příjemcům atd.)

06. Řízení přístupu - udělování oprávnění p

07. Poučení zaměstnanců o ochraně osobn

NOVĚ:

08. Jmenování pověřence pro ochranu oso

09. Zveřejnění kontaktních údajů pověřen

Metodiky k pověřenci:
Metodika Ministerstva vnitra
Pokyn pracovní skupiny WP 29 [evrops

Pověřence pro ochranu osobních údajů musí v souladu s obecným nařízením jmenovat každá obe
zaměstnance obce (nemusí být na celý úvazek, může vykonávat vedle činnosti pověřence i jiné
pověřence nakoupit od externího subjektu. Popřípadě může jednotlo pověřence sdílet více obcí naj

Pověřenec poskytuje obci metodickou podporu, konzultace a školení a posuzuje soulad činnosti o
osobních údajů. Je též kontaktní osobou pro Úřad pro ochranu osobních údajů.

Pověřenec nezodpovídá za ochranu osobních údajů, zodpovědná je obec jako správce. Pověřenec
Nesmí být proto ve střetu zájmů - tedy nemůže současně stanovit systém ochrany osobních úd
Není však vyloučeno, aby plnil i jiné úkoly, které s funkcí pověřence nekolidují, zejména bude-li t
část úvazku dosavadního zaměstnance obce.

K podrobnostem viz metodiku Ministerstva vnitra: http://www.mvcr.cz/gdpr/soubor/metodicke-d
obci-k-organizacne-technickemu-zabezpeceni-funkce-poverence-pro-oou-dle-obecneho-narizeni-o-o
obci.aspx

NOVĚ:

10. Plnění povinnosti hlásit porušení zabezpečení ochrany osobních údajů ÚOOÚ.

Systémová analýza

! Provedení systémové analýzy není povinnost !

Obcím lze doporučit, aby před 25. květnem provedly inventuru zpracování osobních údajů. Jde však o doporučení postupu odpovídajícího praxi zodpovědného správce, nikoli o povinnost.

Složitost a forma inventury záleží na velikosti obce. Inventuru lze zvládnout vlastními silami. Navazovat by na ni měly úpravy vnitřních předpisů, revize souhlasů a zpracovatelských smluv, vždy dle potřeby a s možností využít vzorové dokumenty.

Řada starostů má systémovou analýzu ochrany osobních údajů takříkajíc v hlavě.

Lze ale využít i vzorovou analýzu, kterou MV v rámci své koordinační role nakoupilo pro využití obcemi.

Systémová analýza

Systémovou analýzu připravila Pražská znalecká kancelář, s.r.o. na vzorku 15 obcí.

Dokument je členěn na 2 bloky (pro obce 1. a 2. typu a pro obce s rozšířenou působností) a obsahuje:

- analýzu rizik,
- doporučená řešení modelových situací,
- vzorový časový plán přípravy na GDPR,
- přílohy, zejména přehled agend s uvedením právních titulů zpracování osobních údajů.

Analýza rizik

Analýza rizik vychází z metodologie používané v oblasti kybernetické bezpečnosti.

Identifikuje aktiva (úložiště, agendy, aplikace) a hodnotí jejich váhu.

Určuje hrozby a pro jednotlivá aktiva stanovuje jejich pravděpodobnost.

Určuje zranitelnost aktiv hrozbami.

Výsledkem je rizikové skóre.

Analýza rizik - aktiva

Listinné úložiště v rámci výkonu agend úřadu (L) – veškeré listiny, které jsou uloženy na úřadě a souvisí s výkonem agend úřadu;

Listinné úložiště v rámci vnitřního chodu úřadu (L) – veškeré listiny, které jsou uloženy na úřadě a souvisejí s vnitřním chodem úřadu (příjem a propuštění zaměstnanců, účetnictví atd.);

Informační systém spisové služby (E);

Agendové informační systémy – samostatná působnost (E);

Agendové informační systémy – přenesená působnost (E);

Ekonomický informační systém (E);

Portály – veřejné i neveřejné webové portály (E);

Ostatní elektronická úložiště (E) – e-mail, sdílené disky, lokální disky na počítačových sestavách.

Analýza rizik - hrozby

Příklad – pravděpodobnost hrozeb pro AIS v samostatné působnosti.

Vnější útoky	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Agendový informační systém u obcí se základním rozsahem je většinou hostovaný informační systém, který je dobře chráněn. Atraktivitu pro vnější útoky snižuje také menší objem osobních údajů, které mají obce se základním rozsahem k dispozici.
Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň pravděpodobnosti byla Zhotovitelem stanovena z důvodu nízké pravděpodobnosti selhání technického zajištění AIS – samostatná působnost. Na obcích se základním rozsahem technické chyby nejsou častým jevem.
Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce se základním rozsahem nemají pevně stanovené procesy prací s agendovými informačními systémy např. interními akty.
Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích se základním rozsahem přenesené působnosti Zhotovitel nepředpokládá častější uplatnění dané hrozby.
Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Přístupy do agendových informačních systémů jsou jen v úzkém kruhu zaměstnanců obcí či úřadu.

Analýza rizik - hrozby

Příklad – AIS v samostatné působnosti - zranitelnost aktiva hrozbami.

Vnější útoky	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana Agendového informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno.
Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana AIS je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno. AIS jsou ochráněny před technickými chyby, které by mohli nastat a nedochází ke ztrátě či zcizení dat.
Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
Narušení integrity OU	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na omezený počet zaměstnanců obce či úřadu, který mají přístupy do AIS a nedochází k časté fluktuaci osob mající přístupy do AIS. Zároveň obce nedisponují aktivním řízením přístupů do AIS včetně monitoringu těchto přístupů.

Analýza rizik - skóre

Hodnota aktiva x pravděpodobnost hrozby x zranitelnost hrozbou.

Aktivum	Hodnota aktiva	Rizikové skóre								*Indikátor celkové míry rizika aktiva*
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta osobních údajů	Narušení práv a svobod subjektu údajů	
Listinné úložiště v rámci výkonu agend úřadu	5	30	15	60	45	30	30	60	60	330
Listinné úložiště v rámci vnitřního chodu úřadu	3	18	9	36	27	18	18	36	36	198
Informační systém spisové služby	5	20	50	30	40	20	45	60	45	310
Agendové informační systémy - samostatná působnost	5	20	40	40	30	45	45	45	45	310
Agendové informační systémy - přenesená působnost	5	30	20	20	40	45	30	30	45	260
Ekonomický informační systém	5	30	30	45	15	30	60	30	45	285
Portály	3	27	12	18	9	12	36	18	27	159
Ostatní elektronické úložiště	1	6	10	12	12	12	6	12	12	82
Indikátor celkové míry rizika hrozby	-	181	186	261	218	212	270	291	315	-

Modelová řešení

Systémová analýza obsahuje zásobu doporučení k řešení konkrétních situací. MV ji proto předložilo ÚOOÚ, který materiál v krátkém čase posoudil. Proběhlo jednání MV, ÚOOÚ a dodavatele. Po drobných úpravách a s jistou prodlevou byla analýza zveřejněna.

Diskuse s ÚOOÚ a dodavatelem se týkala například přístupu ke zveřejňování fotografií z obecních akcí. ÚOOÚ zastává právní názor umožňující poměrně pružná řešení. Neexistuje však ještě ustálená výkladová praxe.

Systémová analýza je proto opatrnější. Je možné, že praxe najde jednodušší řešení, nicméně analýza ukazuje bezpečnou cestu.

Jak systémovou analýzu používat

Jak používat systémovou analýzu:

- Nemá smysl ji pouze zkopírovat a prohlásit za svou. Doporučuje se seznámit se s analýzou a posoudit, které její části budou pro obec použitelné, a dále s nimi samostatně pracovat.
- Analýza rizik nezhodnocuje, kde je co špatně, ale ukazuje, jakou intenzitu zabezpečení vyžaduje to které úložiště, agenda nebo aplikace. Může ji zpracovat třeba pověřenec, ale není to povinnost.
- Modelové příklady – nabízejí se k volnému použití. Představují bezpečná řešení z hlediska GDPR s ještě únosnou mírou zátěže.
- V přílohách se zvlášť projevuje, že analýza vychází z dotazníků vyplněných vzorovými obcemi. Seznam agend lze využít při vlastní inventuře osobních údajů, ale je možné, že obec 1. stupně najde některou agendu třeba v příloze pro obce 2. stupně.

Metodika ke spisovým službám

Ministerstvo vnitra zveřejnilo základní metodiku k aplikaci GDPR ve spisových službách.

Důležité je upozornění na význam skartačních lhůt:

- během skartační lhůty trvá právní důvod zpracování osobních údajů; povinnost vymazat osobní údaje neznamená, že je například potřeba se jich zbavit hned po vydání rozhodnutí, ale písemnosti se uchovávají po skartační lhůtu, která buď vyplývá z právních předpisů (MV zveřejnilo jejich přehled), nebo ji stanoví původce se zřetelem k povaze věci (např. s ohledem na lhůty pro mimořádné opravné prostředky, kontrolní činnost nebo promlčecí dobu);
- po uplynutím skartační lhůty musí být provedeno skartační řízení – odevzdání písemností archivu nebo jejich zničení.

Vzorové dokumenty

Ministerstvo vnitra začalo vydávat vzorové záznamy o činnostech zpracování. Jedná se o přehledy základních informací o zpracování osobních údajů v jednotlivých agendách (např. volby, evidence obyvatel, personalistika, smluvní vztahy). Záznamy jsou určeny pro interní potřebu a nezveřejňují se.

K vydání se připravuje jednoduchá interní směrnice o zpracování osobních údajů pro malé obce.

Součástí metodiky k pověřencům pro ochranu osobních údajů je jejich vzorová pracovní náplň.

Záznamy o činnostech zpracování

Záznam o činnostech zpracování - VOLBY
Čl. 30 odst. 1 obecného nařízení o ochraně osobních údajů (GDPR)

Správce: … *(název, adresa, datová schránka)* …
Zástupce správce: …*(jméno, příjmení, funkční zařazení osoby odpovědné za agendu)*…
Pověřenec pro ochranu osobních údajů: … *(jméno, příjmení, e-mail)* …

I. Účely zpracování

ZAJIŠTĚNÍ AGEND OBCE PODLE VOLEBNÍCH ZÁKONŮ

Čl. 6 odst. 1 písm. c) GDPR - zpracování nezbytné pro plnění právní povinnosti:

zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů,
zákon č. 130/2000 Sb., o volbách do zastupitelstev krajů a o změně některých zákonů,
zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů,
zákon č. 62/2003 Sb., o volbách do Evropského parlamentu a o změně některých zákonů,
zákon č. 275/2012 Sb., o volbě prezidenta republiky a o změně některých zákonů (zákon o volbě prezidenta republiky),
prováděcí právní předpisy k volebním zákonům.

II. Kategorie subjektů údajů

Občan obce – volič. Člen okrskové volební komise. Kandidát. Zmocněnec. Petent.

Záznamy o činnostech zpracování

III. Kategorie osobních údajů
Základní identifikační údaje, státní občanství, volební právo a jeho případné omezení, číslo dokladu totožnosti, účast při hlasování; v případě členů okrskových volebních komisí údaje nezbytné pro výkon činnosti člena komise a pro jeho odměňování; v případě kandidátů a zmocněnců identifikační údaje dle kandidátní listiny a čestného prohlášení kandidáta; v případě petentů u nezávislých kandidátů identifikační údaje dle náležitostí petice.
IV. Kategorie příjemců
Členové okrskových volebních komisí pro účely plnění jejich povinností podle volebních zákonů. Kontrolní orgány (krajský úřad, Státní volební komise). Zhotovitel hlasovacích lístků.
V. Plánované lhůty pro výmaz kategorií osobních údajů
Platí skartační lhůty stanovené vyhláškami k volebním zákonům: ve vztahu ke kandidátním listinám a souvisejícím dokumentům - A10, pro ostatní volební dokumentaci - V5.
VI. Obecný popis technických a organizačních bezpečnostních opatření
Listinná vyhotovení volební dokumentace jsou ukládána v uzamčených prostorách a v průběhu voleb se pečetí. Přístup k elektronickým datovým souborům je zabezpečen hesly v souladu s nastavením přístupových práv vnitřními předpisy obce.

Metodika k pověřenci

Ministerstvo vnitra již v roce 2017 vydalo základní metodický návod jak v praxi obcí ustavit pověřence pro ochranu osobních údajů (čl. 37 a násl. GDPR). K 19.2.2018 byl aktualizován.

Pověřence musejí mít obce jako orgány veřejné moci. Dále jej musí jmenovat například školy a některá školská zařízení.

Pověřence nebudou muset mít obslužné organizace.

Pověřenec může být zaměstnancem, nebo lze jeho činnost nakoupit jako službu.

Pověřencem může být fyzická osoba i právnická osoba. Pověřencem může být jmenován např. i svazek obcí, sdružení obcí, jiná obec. Obec může být pověřencem svým příspěvkovým organizacím. Smlouva s externím pověřencem bude vždy nepojmenovanou smlouvou podle občanského zákoníku.

Metodika k pověřenci

Úkoly pověřence:

- poradenská a konzultační činnost pro správce osobních údajů,
- prověřování souladu s GDPR, doporučování opatření k nápravě,
- pomoc při řešení konkrétních situací (zavádění nového zpracování, příprava dokumentace, řešení incidentů, vyřizování podání subjektů údajů),
- kontakt s ÚOOÚ,
- přijímání podání subjektů údajů.

Součástí metodiky je vzorová pracovní náplň pověřence.

Metodika k pověřenci

K častým dotazům:

- Není stanovena kvalifikace pověřence v podobě konkrétního vzdělání. Pověřenec musí být znalý pravidel ochrany osobních údajů a rozumět situaci příslušného správce. Neexistuje státem garantovaná certifikace pověřenců.
- Starosta nemůže dělat pověřence své obci. Sousední obci však ano.
- Zaměstnanec, který zpracovává osobní údaje, není ještě ve střetu zájmů. Pokud nerozhoduje o účelech a prostředcích zpracování a o zabezpečení údajů, může být pověřencem.
- Pověřence lze sdílet. Údaj o 10 obcích na pověřence byl ilustrací. Neexistuje takový limit.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

DĚKUJEME ZA POZORNOST